

Manual básico de administración de docker/squid

Observaciones:

Se proporcionará usuario administrativo para acceso vía SSH.

Desde este punto **squid** es el nombre del contenedor.

1. Listando contenedores

Podemos comprobar los contenedores que están en ejecución:

```
$ docker ps
```

2. Detener y levantar contenedores

Podemos parar o levantar un contenedor:

```
$ docker stop squid
```

```
$ docker start squid
```

3. Ingresar a contenedor docker/squid

Entrar a un contenedor Docker con Bash

```
$ docker exec -it squid bash
```

Verificación de *registros de acceso* del servidor proxy

```
$ docker exec -t squid tail -f /var/log/squid/access.log
```

También se puede ver por la web en el enlace siguiente:

<http://ServerName/squid-reports/>

Verificación de la *lista de control de acceso* al servidor proxy

```
$ docker exec -it squid vim.tiny /etc/squid/squid.acl.conf
```

4. Lista de control de acceso en squid

El archivo principal del servicio squid se encuentra en la siguiente ejecución:

```
$ docker exec -it squid vim.tiny /etc/squid/squid.acl.conf
```

Regularmente una lista de control de acceso se establece siguiendo la siguiente sintaxis:
acl [nombre de la lista] src [lo que compone a la lista]

Ejemplo por rango de direcciones IP:

```
acl miredlocal src 192.168.1.0/255.255.255.0
```

Ejemplo por invocación de fichero:

```
acl permitidos src "/etc/squid/permitidos"
```

Crear el archivo "permitidos"
docker exec -it squid vim.tiny /etc/squid/permitidos

El fichero /etc/squid/permitidos contendría algo como:

```
192.168.1.1  
192.168.1.2  
192.168.1.3  
192.168.1.15  
192.168.1.16  
192.168.1.20  
192.168.1.40
```

5. Reglas de Control de Acceso

La sintaxis básica es la siguiente:

```
http_access [deny o allow] [lista de control de acceso]
```

En el siguiente ejemplo consideramos una regla que establece acceso permitido a Squid a la Lista de Control de Acceso denominada permitidos:

```
http_access allow permitidos
```

En el siguiente ejemplo se establece acceso a Squid a lo que comprenda lista1 excepto aquello que comprenda lista2:

```
http_access allow lista1 !lista2
```

6. Restricción por expresiones regulares.

Para restringir el acceso por dominios, se crea un archivo con lista con dominios.

```
docker exec -it squid vim.tiny /etc/squid/dominios-denegados
```

El fichero /etc/squid/permitidos contendría algo como siguiente:

```
www.facebook.com  
facebook.com  
www.twitter.com  
twitter.com  
www.youtube.com  
youtube.com  
  
facebook.com  
twitter.com  
youtube.com
```

En el archivo principal del servicio squid (/etc/squid/squid.acl.conf) se agrega el control de acceso:

```
acl dominios-denegados dstdomain "/etc/squid/dominios-denegados"  
http_access allow localnet !dominios-denegados
```

7. Validación por usuarios

Para que squid realice la validación por usuarios se tiene que añadir la siguiente línea de fichero de configuración:

```
auth_param basic program /usr/lib/squid/basic_ncsa_auth /etc/squid/password
```

/etc/squid/password es el nombre del fichero donde se guardan los usuarios y sus contraseñas. puede cambiarse a gusto del administrador.

Se crea el fichero (opción -c) y se añade el usuario manuel

```
htpasswd -c /etc/squid/password manuel
```

Se añade otro usuario llamado juan. **¡No se debe escribir la opción -c de nuevo porque se destruye el archivo que haya!**

```
htpasswd /etc/squid/passwd juan
```

Nota: si se quiere modificar la contraseña de usuario una vez que se ha añadido, se puede hacer usando la opción -c puesto que se detecta la existencia del usuario y no destruye el fichero que había.

Luego, las reglas han de definirse utilizando la palabra reservada proxy_auth, como puede observarse en el ejemplo:

#lista control de acceso

```
acl permitidos proxy_auth manuel
```

#lista de acceso

```
http_access allow permitidos
```

```
http_access deny all
```

Recargar la configuración del servicio para aplicar cambios

```
docker exec -it squid service squid restart
```